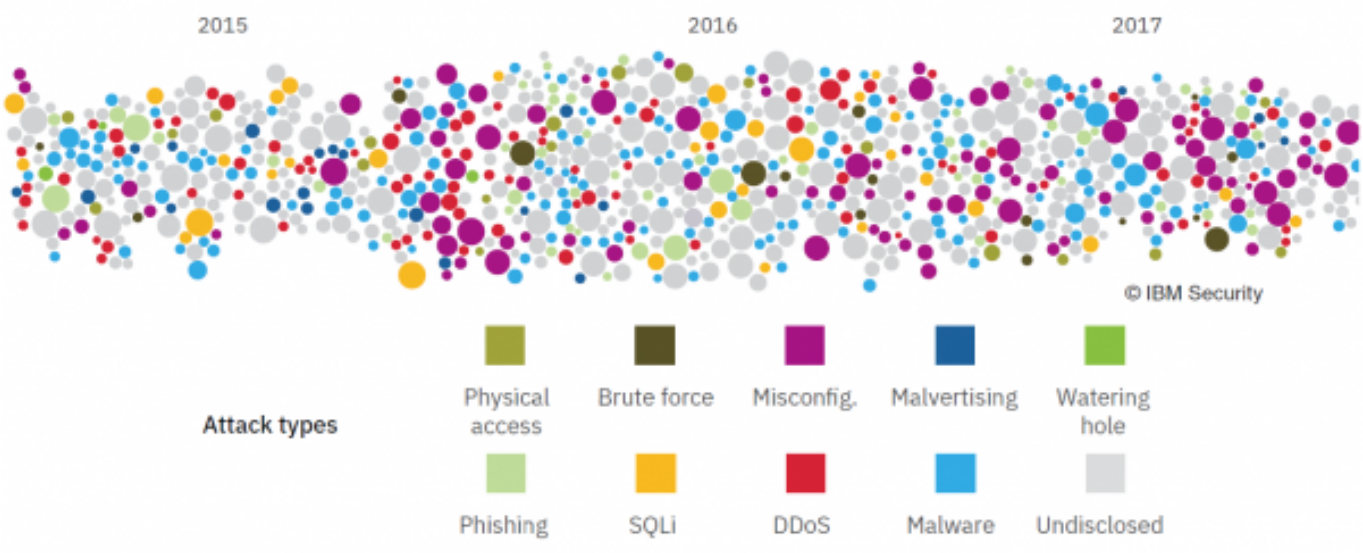


x-force report IBM Security c IBM

Doch in diesem Artikel richtet sich das Augenmerk auf den Faktor menschliches Versagen im hektischen Alltag. Hierbei ist die Abgrenzung von „menschliches Versagen durch Unachtsamkeit im hektischen Alltag" zu „menschliches Versagen durch fachliche Nachlässigkeit" nicht so einfach.

von Isabella Pridat-Zapp

Der IBM X-Force Threat Intelligence-Index umfasst Erkenntnisse und Beobachtungen aus Daten, die über Hunderte von Millionen von geschützten Endpunkten und Servern in nahezu 100 Ländern analysiert wurden. IBM X-Force unterhält Tausende von Spam-Traps auf der ganzen Welt und überwacht täglich Millionen von Spam- und Phishingangriffen. Dabei werden Milliarden von Webseiten und Bildern analysiert, um betrügerische Aktivitäten und Missbrauch zu erkennen.

Besonders auffällig ist, dass menschliches Versagen im Jahr 2017 für zwei Drittel aller kompromittierten Datensätze verantwortlich war, ebenso für den Rekordanstieg bei falsch konfigurierten Cloud-Infrastrukturen. Unabhängig von dem Vehikel, das für den Zugriff auf fremde Daten genutzt wird, ist also das menschliche Versagen nach wie vor der wichtigste Faktor.

Unter Kosten/Nutzen-Aspekten ist die Analyse und gezielte Bekämpfung der möglichen diesbezüglichen Schwachpunkte ein optimaler Ansatz mit höchster Priorität für Unternehmen und Organisationen. Es ist ja nicht so, dass dieses Ergebnis eine Überraschung darstellt, den bereits im Juni 2014 schrieb das X-Force Team in seinem Halbjahresreport nach Auswertung von fast 1000 Kundensituationen in 133 Ländern, dass 95 Prozent der Attacken in irgendeiner Weise durch menschliches Fehlverhalten Erfolg erzielten.

Neben falsch konfigurierten Clouds und Network-Backups ohne Authentifizierung oder mit schwacher Authentifizierung, machten im Berichtsjahr 2017 die Einzelpersonen, die über Phishing-Attacken gehackt wurden, ein Drittel der Vorfälle zum Thema menschliches Versagen aus, die zu einem Sicherheitsvorfall führten. Dazu gehört das Klicken auf einen Link oder das Öffnen eines Anhangs mit bösartigem Code im Rahmen einer von Cyberkriminellen gestarteten Spam-Kampagne. Bei den meisten erfolgreichen Szenarien war die Voraussetzung eine Fehleinschätzung des primär Angegriffenen. So haben Mitarbeiter das geistige Eigentum ihres Arbeitgebers in Form von Daten auf ihren eigenen unsicheren privaten Geräten gespeichert und Angestellte und Insider wurden Opfer von Phishingkampagnen – mit dem Resultant dass der Angreifer Zutritt und Vollmacht

erlangte und auch sensible Daten herunterladen und unter anderem in Ransom-Szenarien manipulieren konnte.

Angriff per eMail

Besonders gefährdete Wirtschaftsbereiche
© IBM Security

Nach wie vor ist die eMail, trotz der Zunahme von Chat und Instant Messaging Anwendungen, eine der verbreitetsten Kommunikationsmethoden aller Unternehmen und Organisationen und so ist Phishing immer noch die erfolgreichste Zugriffsmethode durch Aussenseiter. Die Phishing-Mail kann den Mitarbeiter auf eine falsche Website führen, wo er in der Annahme, sich auf der Unternehmens-Site zu befinden seine Logdaten eingibt. Nach erlangtem Zutritt erfolgt die Übernahme von Website-Accounts mit allen dort gespeicherten Zugriffsdaten und der Möglichkeit, falsche Eingabebildschirme zu generieren und weitere User und deren Zugriffsdaten zu kompromittieren. Der Angreifer erlangt somit alle Berechtigungen aller kompromittierten Nutzer. Stark zugenommen haben in den letzten Jahren auch sogenannte BEC Angriffe (Business Email Compromise), die auch unter dem Begriff CEO Fraud bekannt sind.

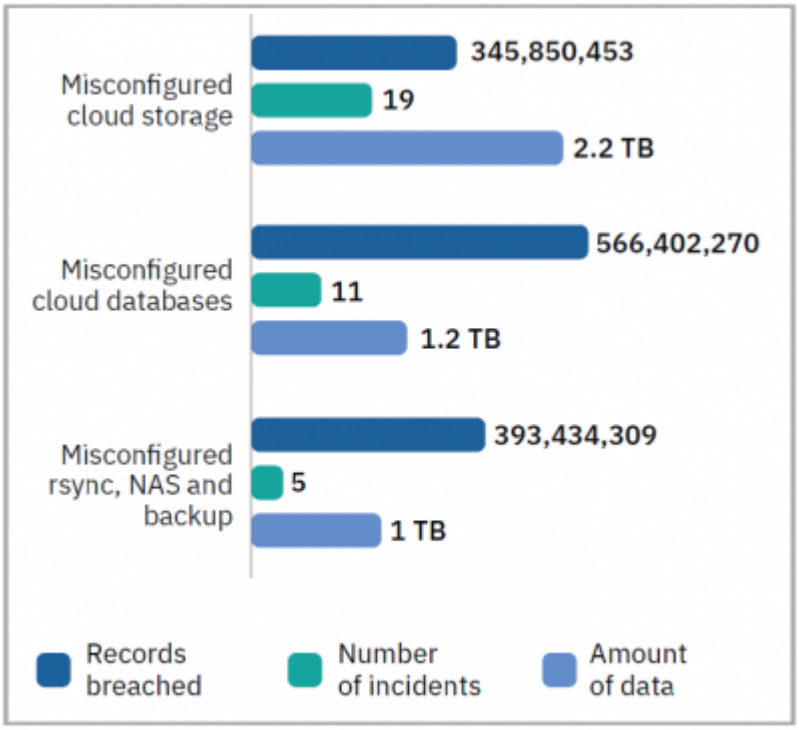
Ein beliebtes Media-Hosting Unternehmen erlag so zum Beispiel einem Phishing-Angriff bei dem der Angreifer 3.12 TB interner Daten erhielt. Im Gesundheitssektor wurde durch Phishing Attacken bei mehreren Kliniken Zugriff auf die eMail Accounts der Angestellten erlangt und somit auf die dort enthaltenen vertraulichen Patientendaten.

Phishing-Mails mit oder ohne zu clickende Links (lt. Report in 2017: 38% der beobachteten Insider-Fälle) und/oder deren Malware-Mail-Anhänge sind inzwischen sehr überzeugend gestaltet, so dass der Empfänger sie nicht als Angriff erkennt. Als lukrativste Methode scheinen sich die oben erwähnten BEC-Angriffe erwiesen zu haben, die in den letzten Jahren stark zugenommen haben. Diese Phishing-Mails geben vor, von dem Eigentümer des Unternehmens, dem CEO oder einem anderen sehr einflussreichen Geschäftsleitungsmitglied zu stammen und fordern den Empfänger

meistens auf, Überweisungen sehr großer Beträge als vorgebliche Zahlung vorzunehmen.

Durch BEC-Angriffe entstand laut dem Report im Laufe von 3 Jahren weltweit ein Schaden von über 5 Milliarden US$ (Okt. 13 bis Dez. 16). Im Jahr 2017 gelang es durch einen BEC-Angriff, eine kanadische Universität zur Überweisung von 11,4 Millionen kanadischen Dollars zu veranlassen. Auch hier gelang der initiale Zutritt durch eine eMail und einen ahnungslosen Mitarbeiter, der es versäumt hat, sich der Echtheit der Anweisung intern zu vergewissern.

Ungeschützte private Geräte



Konfigurations-Fehler
© IBM Security

Ein weiteres Beispiel für die Gefährdung des Arbeitgebers durch Angestellte boten im vergangenen Jahr wieder Mitarbeiter, die Unternehmensdaten auf ihre persönlichen Geräte kopiert haben. In einem dieser Fälle arbeitete ein Angesteller der US-Regierung auf seinem nicht gesicherten privaten PC mit einer Fallmanagement-Anwendung. So wurden unbeabsichtigt die persönlichen Daten von 247.167 Personen kompromittiert. Ferner erlangten die Angreifer Zugriff auf vertrauliche Ermittlungsberichte aus den Jahren 2002 bis inclusive 2014, aus denen die betroffenen Personen, die Zeugen und auch Beschwerden an die Personalabteilung hervorgingen.

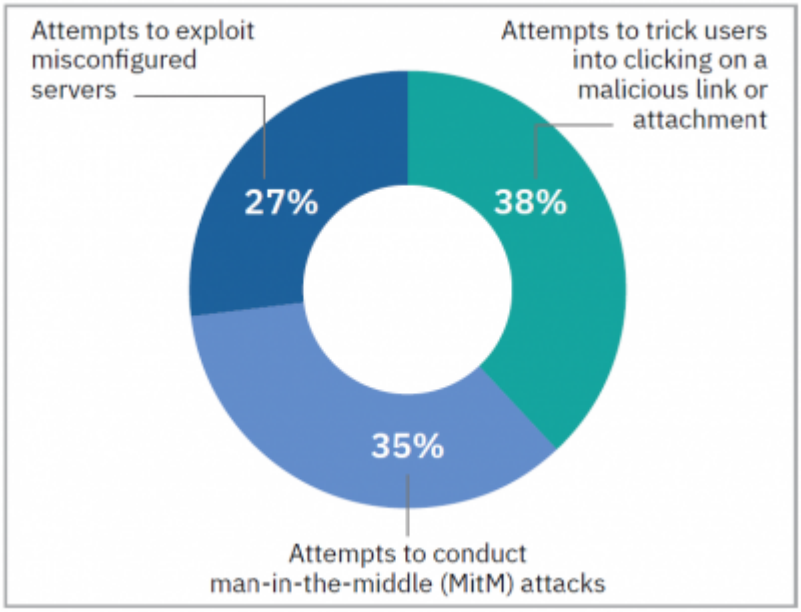
Als weitere Quelle des Gefährdungsanstiegs benennen die Autoren der X-Force Studie den zunehmenden Einsatz von Malware auf mobilen Geräten. Angesichts zunehmender Nutzung von mobilen Zahlungen, Shopping-Anwendungen und Mobile Banking macht sich die Cybercrime-Szene bereit, den Konsumenten vermehrt anzugreifen, so dass in diesem Bereich 2018 mit mehr Schäden zu rechnen ist. Die Verbreitung von Banking Trojanern und deren Codes in offiziellen App Stores im Android Bereich hat weltweit zugenommen.

MitM-Attacken

Auch bei den sogenannten MitM-Attacken (35%) setzen die Angreifer auf unaufmerksame oder schlecht informierte Opfer. Bei einem solchen „Man in the middle“-Angriff würde beispielsweise jemand versuchen, sich über einen kompromittierten Wi-Fi Router mit einer Bank-Website zu verbinden und dann die Warnmeldung zum Sicherheits-Zertifikat ignorieren und übergehen. Wenn sich das Opfer nun einloggt, werden die LogIn-Daten an den Angreifer gesendet. Bei weiteren 27% der Angriffe handelt es sich um fehlerhaft konfigurierte Server (meist mittels SCLi, SCL injection Angriffe).

Vulnerabilität nach Bereichen

Die Experten von IBM Security weisen im X-Force Report auch darauf hin, dass es wohl Personengruppen gibt, die besonders anfällig für alle Arten von Angriffen sind. Hierbei handelt es sich um Mitarbeiter von Unternehmen und Organisationen der Bereiche Bildung, Energieversorgung, Utilities und Finanzen. Warum das so ist, lässt sich wohl aus den Vorfall-Daten nur vermuten. Es wäre jedoch laut X-Force plausibel, anzunehmen dass diese Bereiche besonders viele Ph



Statistische Verteilung der Angriffs-Methoden © IBM Security

ishing-Mails erhalten, was die Wahrscheinlichkeit erhöht. Der Bildungs-Bereich wurde beispielsweise ganz besonders vielen BEC-Angriffen ausgesetzt. Doch auch mangelndes Gefährdungs-Bewusstsein scheint hier eine Rolle zu spielen, wie eine andere Studie aus dem Jahr 2017 ergab: So gaben 82 % der EDV-Mitarbeiter des Bereichs Bildung an, dass sie von den Studenten ein jährliches Datensicherheits-Training verlangen, während gleichzeitig nur 35 % der Studenten wusste, dass ihre Universität dies verlangt.

In den vergangenen Jahren war die Finanzbranche von Cyberkriminellen mit am stärksten betroffen. Im Jahr 2017 fiel sie zwar auf den dritten Platz in Bezug auf Anzahl der Angriffe (17 Prozent) – hinter der Informations- und Kommunikationstechnologie (33 Prozent) und der Fertigung (18 Prozent) – erlebte jedoch die meisten Sicherheitsvorfälle (27 Prozent), die einer weiteren

Untersuchung bedurften. Weil Finanzdienstleister inzwischen stark in Cybersicherheitstechnologien zum Schutz ihrer Organisationen investiert haben, konzentrieren sich Cyberkriminelle nun darauf, Banking-Trojaner gezielt gegen Endverbraucher und Bankkunden einzusetzen.

Passworte gestern und heute

Weiterführende Literatur:

Um eine Kopie des IBM X-Force Threat Index 2018 herunterzuladen und Zugriff auf die zahlreichen dort genannten Quellen zu erhalten, besuchen Sie bitte: https://www.ibm.com/account/reg/us/signup?formid=urx-31271

Die nächste Ausgabe der NEWSolutions enthält den Beitrag „Unternehmens-Projekt Sicherheit – sich an erfolgten Projekten orientieren“. Für diesen Beitrag wurden die unterschiedlichsten Studien daraufhin untersucht, womit und wie die Unternehmens-Sicherheit für die eigenen Bedürfnisse optimiert werden kann: NEWSolutions 2/2018